In re Appln. of Bishop, et al.
App. No. 10/821,379

REMARKS/ARGUMENTS

Claims 5, 7-12 and 43-50 are pending in the present application. Claims 5, 7-12 and 43-50 stand rejected. Claim 5, 7, 8, 9, 10, 43, 45, 47 and 48 have been amended. No claims have been canceled or added. Reconsideration of claims 5, 7-12, and 43-50 in light of the present remarks is respectfully requested.

Rejections Under 35 U.S.C. § 103

The Examiner has rejected claims 5, 7-12 and 43-50 under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 6,473,794 to Guheen et al. in view of U.S. Patent No. 6,298,444 to Foss et al. Applicants respectfully traverse the rejection.

Claim 5 is directed to a method for protecting a network server from being used as the basis of an attack on a network client. Among other elements, amended claim 5 requires "editing each of said executable commands such that said executable commands will not be executed by the network server." As explained in the specification, a Web site typically includes various pages, each having a unique URL. Users of the site may place an elevated trust in certain servers or certain portions of servers (such as those corresponding to financial institutions or merchants who are reputable). The certain servers or portions of servers in which the elevated trust is placed are referred to as a trusted portion. In the context of reducing or eliminating undesirable executable code, data provided to the trusted portion of a Web site may be monitored for executable code. In one example, scripting languages, such as JavaScript, are frequently encoded with script instructions placed between angle brackets ("<" and ">"). By editing the executable code, for example, to remove the angle brackets, the executable code can be eliminated from the data, thereby reducing, and in some cases, eliminating the security risk to the system. One of the many advantages of eliminating executable code from the data is the system is not dependent on analyzing incoming commands to determine whether they are malicious.

Applicants respectfully submit that neither Guheen, nor Foss, disclose, teach, or suggest editing each of said executable commands such that said executable commands will not be executed by the network server.

Guheen is directed to a system, method and article of manufacture for planning the testing of components in an existing network. The only portions of Guheen directed in any manner towards security management is at column 57, line 44 to column 58, line 51. However, as previously noted, these portions only relate to preventing the transfer of viruses either by defining access rights or isolating the development environment by allowing internet access only via a dial-up connection on stand-alone machines. Accordingly, Guheen does not disclose, teach, or suggest editing each of said executable commands such that said executable commands will not be executed by the network server, as required by claim 5.

Foss is directed to a network security system that prevents unwanted email messages from entering a network by selectively checking portions of the email. Foss fails to disclose, teach, or suggest editing each of said executable commands such that said executable commands will not be executed by the network server, as required by claim 5. Instead, Foss discloses a mail guard device 207, which invokes a rule set to determine whether an incoming e-mail includes characters, symbols (and certain sequences thereof) and commands that are not allowed. If improper content is detected, the improper instructions or operations are translated to appropriate executable instructions and, only if translation is impractical, the instructions are rendered useless. Foss's system specifically does not prevent executable code from being executed in the system, in fact, it makes efforts to ensure all executable code is executed. The present invention, however, provides enhanced security over incoming messages by ensuring that executable commands contained within said messages are rendered inert. Therefore, Foss fails to disclose, teach, or suggest editing each of said executable commands such that said executable commands will not be executed by the network server, as required by claim 5.

As noted above, Guheen and Foss, alone or in combination, fail to disclose, teach, or suggest "editing each of said executable commands such that said executable commands will not be executed by the network server," as required by claim 5. As a result, Applicants respectfully submit that claim 5 is patentable over Guheen in view of Foss. Additionally, claims 7-12 depend from claim 5, and include all the elements of claim 5. Therefore, Applicants respectfully submit that claims 7-12 are also patentable over Guheen in view of Foss.

Claim 43 is directed to a computer-implemented method for protecting a network server from being used as the basis for an attack on a network client. Similar to claim 5, among other elements, claim 43 requires "removing each of said executable commands such that the security risk posed by said executable commands is climinated." As explained in the specification, a Web site typically includes various pages, each having a unique URL. Users of the site may place an elevated trust in certain servers or certain portions of servers (such as those corresponding to financial institutions or merchants who are reputable). The certain servers or portions of servers in which the elevated trust is placed are referred to as a trusted portion. In the context of reducing or eliminating undesirable executable code, data provided to the trusted portion of a Web site may be monitored for executable code. In one example, scripting languages, such as JavaScript, are frequently encoded with script instructions placed between angle brackets ("<" and ">"). By editing the executable code, for example, to remove the angle brackets, the executable code can be eliminated from the data, thereby reducing, and in some cases, eliminating the security risk to the system. One of the many advantages of eliminating executable code from the data is the system is not dependent on analyzing incoming commands to determine whether they are malicious. The present invention, therefore, provides enhanced security over incoming messages by ensuring that executable commands contained within said messages are rendered inert.

As noted above with respect to claim 5, both Guheen and Foss fail to disclose, teach, or suggest "removing each of said executable commands such that the security risk posed by said executable commands is eliminated," as required by claim 43. As a result, Applicants respectfully submit that claim 43 is patentable over Guheen in view of Foss. Additionally, claims 44-50 depend from claim 43, and include all the elements of claim 43. Therefore, Applicants respectfully submit that claims 44-50 are also patentable over Guheen in view of Foss.

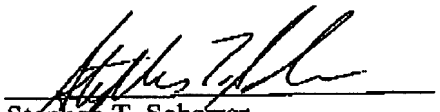
In re Appln. of Bishop, et al.
App. No. 10/821,379

CONCLUSION

In view of the foregoing remarks, Applicants respectfully submit that all of the claims in the Application are in allowable form and that the Application is in condition for allowance. If, however, any outstanding issues remain, Applicants respectfully urge the Examiner to telephone Applicants' undersigned attorney so that the same may be resolved and the Application expedited to issue. Applicants respectfully request the Examiner to indicate all claims as allowable and to pass the Application to issue.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP



Stephen T. Scherrer
Registration No. 45,080

Please recognize our Customer No. 1923 as our correspondence address.

227 West Monroe Street
Chicago, IL 60606-5096
Phone: 312.372.2000
Facsimile: 312.984.7700
Date: October 24, 2007

CHI99 4894651-1.037355.0239